



# U.S. Chemical Safety and Hazard Investigation Board

**SUBJECT:** Personnel Suitability and Security Program

---

## CONTENTS

1.	Purpose .....	2
2.	Effective Date.....	2
3.	References .....	2
4.	Scope .....	2
5.	Definitions.....	2
6.	Relationship Between Suitability and Security .....	5
7.	Responsibilities .....	6
8.	Orientation and Information for Employees .....	10
9.	Suitability .....	10
10.	Computer/IT Risk Criteria and Levels.....	15
11.	National Security Positions .....	18
12.	Personnel Investigations.....	24
13.	Recordkeeping .....	25
14.	Review and Update .....	25
	Appendix A Risk Designation System	
	Appendix B Form and Investigation Matrix	
	Appendix C Position Designation Record	

1. **PURPOSE.** This Order establishes policies and standard operating procedures for the Chemical Safety and Hazard Investigation Board’s (CSB) personnel security and suitability program.
  2. **EFFECTIVE DATE.** This Order is effective upon passage by the Board.
  3. **REFERENCE.** This Order implements the requirements of Executive Order 10450, “Security Requirements for Government Employment,” as amended; Executive Order 12968, “Access to Classified Information;” Executive Order 10577, “Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service;” 5 Code of Federal Regulations (CFR) Parts 731, 732, and 736; and Homeland Security Presidential Directive Number 12 (HSPD-12). Additional references include Public Law 108-458 (The Intelligence Reform and Terrorism Act of 2004); Executive Order 13381, “Strengthening Processes Relating to Determining Eligibility for Access to Classified Information,” NIST FIPS 201-1 – Personal Identification Verification (PIV) of Federal Employees and Contractors, March 2006; Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Pub. L. 104-208, 110 Stat. 3009; Office of Management and Budget Memorandum M-07-21; and the Privacy Act of 1974, as amended. In the case of any inconsistency between this Order and any federal statute or regulation, the federal statute or regulation shall govern.
  4. **SCOPE.** This Order is applicable to all CSB employees. It is also applicable to a contractor employee who will require a clearance for access to classified national security information (classified information) to perform his or her duties at the CSB. Other categories of workers will be subject to background investigations based on whether they will be acting as a representative of the CSB, or if they require CSB IT system access or CSB facility access.
  5. **DEFINITIONS.**
    - a. *Access* – (1) The ability and opportunity to obtain knowledge of classified information. An individual is considered to have access to classified information if he/she is admitted to an area where such information is kept or handled and security measures do not prevent that individual from gaining knowledge of such information. (2) The ability and means to approach, store or retrieve data, or to communicate with or make use of a resource of an automated data processing system. (3) A condition or equipment mode that allows authorized entry into a protected area without alarm by electronically or mechanically deactivating a sensor or sensors.
    - b. *Adjudication* - Examination of a sufficient period of a person’s life to make an affirmative determination that the person is suitable for the responsibilities of his Federal position or eligible to hold a security clearance.
    - c. *Alien* - Any person not a citizen or national of the United States.
    - d. *Applicant* – A person who has applied, and is being considered, for Federal employment.
-

- e. *Appointee* – A person who has entered on duty and is in the first year of the appointment to a position that is subject to investigation.
- f. *Classification* – The act or process by which information is determined to be classified information under E.O. 12958, Classified National Security Information.
- g. *Classified National Security (classified information)* – Information that has been determined pursuant to E.O. 12958, Classified National Security Information, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
- h. *Compromise* – A probable compromise occurs when (1) classified material is recovered outside of a controlled area or (2) when the controlled area or facility is unattended and not properly secured. In either case, a compromise occurs when the material is accessible to persons who do not possess an appropriate security clearance or a need-to-know. An actual compromise occurs when with the conditions identified above, it is determined that the classified information has been released or disclosed to an unauthorized person(s) or party(s), and that damage to national security is deemed likely or determined to have occurred as the result of this unauthorized disclosure. A probable compromise of classified information occurs whether the act was intentional or unintentional.
- i. *Covered Position*- A position in the competitive service, a position in the excepted service where the incumbent can be noncompetitively converted to the competitive service (for example, the Federal Career Intern Program), and a career appointment to a position in the senior executive service.
- j. *Eligibility for Access* – A favorable adjudication of an appropriate investigation of the subject's background.
- k. *Employee* - A person who has completed the first year of appointment to a position that is subject to investigation.
- l. *Entrance on Duty (EOD)* – The first day that a person enters employment or reports to his/her duty station for work.
- m. *Electronic Questionnaires for Investigations Processing (e-QIP)* – A web-based automated system that has been developed by OPM, Center for Federal Investigative Services, and approved by the Office of Management and Budget (OMB) for public use, to provide a means to facilitate the processing of the questionnaires for background investigations commonly known as Standard Forms (SF) SF-86, SF-85P, or SF-85.
- n. *High Risk (HR) Public Trust Positions* – Positions with the potential for exceptionally serious impact on the efficiency of the service.

- o. *I-9 Approved Identification* - A form of identification that is identified on a list of acceptable documents on Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document must be a valid State or Federal government-issued picture ID.
- p. *Identity-Proofing* - The process of providing sufficient information (e.g., driver's license, proof of current residence, etc.) to a registration authority, or the process of verifying an individual's information that he or she is that individual and no other.
- q. *Low Risk or Non-Sensitive Positions* – A position that has the potential for impact involving duties of limited relation to the agency mission or national security, with program responsibilities that affect the efficiency of the service.
- r. *Moderate Risk (MR) Public Trust Positions* – A position with the potential for moderate to serious impact on the efficiency of the service.
- s. *National Security* - The national defense or foreign relations of the U.S. (refer to E.O. 12958).
- t. *Non-Employees* – Individuals employed by the CSB, or allowed to perform services directly to the CSB, but who do not fall under Career, Career Conditional, SES, Schedule C, or Excepted Service status. Examples are Advisory Committee Members, Guest Workers, Research Associates, Experts, Consultants, Long-Term Visitors and Interns (unpaid). Does not include contractors.
- u. *Personal Identity Verification (PIV)* – A process required by HSPD-12 to ensure that individuals issued Federal identity cards are only issued cards after presenting secure and reliable forms of identification, and at a minimum that a National Agency Check with Inquiries (NACI) type investigation has been conducted or initiated.
- v. *Public Trust Positions* - Generally positions in which the duties or responsibilities involve policy making; major program responsibility; public safety and health; law enforcement duties; fiduciary responsibilities; and other activities demanding a significant degree of public trust. Such positions also involve access to, operation or control of proprietary systems of information, such as financial or personnel records, with a significant risk for causing damage to people, programs or an agency, or realizing personal gain.
- w. *Risk Designation System* - The basic system explained in Section 9 that determines department, program, and position placement based on general risk level criteria for all positions at the CSB from both a public trust and national security standpoint.
- x. *Sensitive-But-Unclassified (SBU)* – A category of information managed by the CSB that is not considered vital to the national security, but the indiscriminant disclosure of which would do some harm. This type of information falls under one of the nine exemptions to the Freedom of Information Act (FOIA). See the CSB's FOIA policies

and procedures at 40 C.F.R. § 1601,  
<http://safetynet/docs/GC/regulations/FOIARegulation.pdf>.

- y. *Suitability* – Identifiable character traits and past conduct, which are sufficient to determine whether an individual is likely or unlikely to be able to carry out the duties of the job with appropriate efficiency and integrity. It also refers to statutory or regulatory bars, which prevent the lawful employment of the individual in the position.
- z. *Trustworthiness* – Security decision with respect to extended investigations to determine and confirm qualifications, and suitability to perform specific tasks and responsibilities.

6. **RELATIONSHIP BETWEEN SUITABILITY AND SECURITY.**

- a. Suitability means fitness or eligibility for employment and refers to identifiable character traits and past conduct that are sufficient to determine whether a given individual is likely or not likely to be able to carry out the duties of a Federal job with appropriate efficiency and effectiveness. Suitability is distinguishable from a person's ability to fulfill the qualifications requirements of a job, as measured by experience, education, knowledge, skills, and abilities. Suitability adjudication focuses on whether the employment or continued employment of an individual can reasonably be expected to promote the efficiency of the Federal service. Title 5 CFR Part 731 contains potentially disqualifying suitability factors for competitive service and certain excepted service employees and states the circumstances under which persons may be disqualified for employment for suitability reasons.
- b. Security relates to requirements for an individual occupying a specific position to have access to classified information. A security determination focuses on the question of whether or not access to such information is clearly consistent with the interests of the national security.
- c. In processing applicants for employment, a security determination under E.O. 10450 and/or E.O. 12968, will usually be made subsequent to favorable suitability determination. Therefore, the CSB may favorably adjudicate a background investigation or information the applicant has provided, and find the person suitable for employment in a specific position, but then separately determine whether or not the person should have access to classified information. In the case of an employee, however, neither suitability determination nor a security determination is contingent upon the other. For example, a security determination may result in reassignment or removal from a position under the provisions of this Order, even if there has been no suitability determination. Also, those provisions, in which a security determination precludes an employee from being granted a security clearance, could prevent the promotion or reassignment of the employee to a sensitive position.

## **7. RESPONSIBILITIES.**

### *a. Chairperson:*

In consultation with the General Counsel, HRD, and Chief of Personnel Security and the concurrence of the reviewing Board Member (as designated under Board Order 010), is authorized to:

1. Suspend or remove an employee for security reasons, pursuant to Section 5.2(6) of E.O. 12968, 60 Federal Register 40245, 40252 (August 7, 1995).
2. Restore to duty an employee who was suspended or removed under 5 U.S.C. Section 7532.
3. Make suitability determinations for Schedule C or Non-Career Senior Executive Service (SES) applicants or appointees.
4. May approve the waiver of the pre-appointment background investigation requirement for appointments to critical-sensitive national security positions.
5. Impose a period of debarment of up to three years from all or specific competitive service positions, and other appropriate positions within the CSB, in accordance with OPM regulations and guidance and the CSB policies and procedures, and impose a cancellation of pending applications in any case in which an ineligible or removal decision has been made under 5 CFR 731, or HSPD-12.
6. Take unfavorable action against an applicant, appointee, or employee in accordance with 5 CFR 732 or 315.
7. Initiate appropriate action against appointees, employees or non-employees upon notification that, the CSB could not make a favorable suitability determination or could not grant a national security clearance to an appointee, employee, or non-employee.

### *b. Chief of Personnel Security:*

1. Ensures effective implementation of E.O. 12968, “Access to Classified Information”, or successor policy, concerning the eligibility for access to classified national security information.
2. Grants clearances for access to Classified National Security Information on a need-to-know basis, for any individual employed by the CSB, including non-Federal employees working on a CSB contract, including all subcontractors.

3. Requests and ensures the completion and successful adjudication of required investigations corresponding to position risk or sensitivity levels for all applicants, appointees and employees.
4. Serves as the CSB Program Manager for e-QIP.
5. Consults with the HRD and the General Counsel on the assignment of position risk or sensitivity levels.
6. Maintains active oversight and continuing security education and awareness programs to ensure effective implementation of Executive Order 12968.
7. Conducts periodic evaluations of the implementation of Executive Order 12968.
8. With the approval of the Chairperson and in accordance with applicable law, may enter into an interagency services agreement with a qualified federal agency to obtain support in the execution of the above responsibilities and may delegate to such agency initial adjudicative determinations as outlined in section 3 of this subsection.

c. *Human Resource Director:*

1. Ensures that applicants, appointees and employees comply with the requirements of this order.
2. Ensures that all Optional Form 8's (OF-8), Position Description, either electronic or hard-copy, show the approved sensitivity or risk level designation, as well as any requirement for access to classified information.
3. When appropriate, ensures that vacancy announcements state that appointment is subject to a favorably adjudicated personnel security investigation enabling the granting of a security clearance.
4. Ensures that before placing, or making any commitment to place, a person in a position requiring a clearance for access to classified information, which would be a Critical Sensitive, or Non-Critical Sensitive position, the Chief of Personnel Security has determined that the pre-placement investigative requirement has been met or that an appropriate waiver has been granted.
5. Establishes an employee in the e-QIP system and provide them the e-QIP Quick Reference Guide, if the employee requires a reinvestigation. The e-QIP form to be completed is determined by the position risk or sensitivity level assigned to the position. (See Section 12.b. Personnel Investigation Forms.)
6. Ensures that all announcements for positions at the CSB contain language to indicate that a background investigation may be required on a pre- and/or post-appointment basis. Also, if the background investigation is a post-appointment

requirement, that continued employment will be contingent upon the favorable adjudication of the background investigation.

7. Establishes an applicant in the e-QIP system and provide them the e-QIP Quick Reference Guide as an enclosure with their notification of appointment letter. The e-QIP form to be completed is determined by the Position Risk or Sensitivity level assigned to the position. (See Section 12.b. Personnel Investigation Forms.)
8. Provides the Chief of Personnel Security a copy of the notification of appointment letter, OF-306, Resume and Position Authorization and Description Form (EP-8) with Position Description.
9. Ensures that applicants and appointees are not appointed to positions that are designated Critical Sensitive or Non-Critical Sensitive without appropriate clearance from the Chief of Personnel Security. (See Section 11.e.)
10. Conducts pre-appointment suitability screenings and refers to the Chief of Personnel Security as appropriate for pre-appointment security determinations.
11. Provides necessary assistance with CSB debarments from employment.
12. Ensures that position risk and sensitivity level codes are accurately recorded in official records. This includes the Federal Personnel Payroll System (FPPS), and documents in Official Personnel Folders – Position Authorization and Description (EP-8) and Notification of Personnel Action (SF-50). The Chief of Personnel Security must have approved the position sensitivity code in block #14 on the EP-8 for the employee's position of record; that same code must appear in FPPS, and on the employee's SF-50.
13. Files Certificates of Investigation and certified Requests for Security Officer Action (RSA) forms on the permanent side of the OPF.
14. Reports incidents or situations that may affect Personnel Security or Suitability, or the physical security of employees at the CSB to the Chief of Personnel Security and to the General Counsel.
15. Initiates an appointee, employee, or non-employee as necessary, in e-QIP so that the individual can access the system and complete his/her SF 86, SF 85P, SF 85P-S, or SF 85 electronically, and provide the individual with the e-QIP Quick Reference Guide.
16. Determines suitability for employment of applicants for, or appointees to, positions in the Excepted Service in accordance with OPM regulations and guidance, and the CSB policies and procedures, and providing due process as appropriate.



17. Determines suitability for employment of applicants for, or appointees to, competitive service or career SES positions, in accordance with 5 CFR Part 731 and OPM guidance, and providing due process as appropriate.
18. Evaluates, and approves with the concurrence of the Chief of Personnel Security and the General Counsel, position sensitivity and/or position risk level designations commensurate with the duties and responsibilities related to national security and/or to the efficiency of the service to each CSB position. In consultation with the Chief of Personnel Security and General Counsel, completes a “Position Designation Record” form for each position, to include when changes are made to the position that affect the position’s risk or sensitivity level. (see appendices A and C.)
19. With the approval of the Chairperson and in accordance with applicable law, may enter into an interagency services agreement with a qualified federal agency to obtain support in the execution of the above responsibilities and may delegate to such agency adjudicative responsibility as outlined in section 16 of this subsection.

d. *General Counsel:*

1. Advises the Chairperson on the exercise of the responsibilities described in paragraph 7.a. of this Order.
2. Advises the Chief of Personnel Security on the assignment of position risk or sensitivity levels, as described in paragraph 7.b.5. of this Order.
3. Advises the HRD on position sensitivity and/or position risk level designations, and on the completion of a “Position Designation Record” form for each position, as described in paragraph 7.c.18. of this Order.
4. Receives, along with the Chief of Personnel Security, reports from the HRD on incidents or situations that may affect Personnel Security or Suitability, or the physical security of employees at the CSB.

e. *Office Directors:*

1. Notify the Chief of Personnel Security and the HRD prior to the departure of employees or non-employees, to ensure there is no action required prior to their departure.
2. Report incidents or information that may affect the Personnel Security or Suitability Programs at the CSB to the Chief of Personnel Security.

f. *Applicants, Appointees or Employees:*

1. Complete required forms upon request in e-QIP at [www.opm.gov/e-qip](http://www.opm.gov/e-qip), and provide paper forms as necessary.

2. Appear in person with two forms of government (State or Federal) issued photo identification for purposes of identity verification before the issuance of a PIV credential.

8. **ORIENTATION AND INFORMATION FOR EMPLOYEES.**

- a. Any questions the employee may have regarding the content of this Order or risk designation may be referred to their Supervisor. If an employee wants additional information, he or she may request a briefing from the HRD. After the employee has had a briefing, and questions still remain, the employee may submit those remaining questions in writing to the HRD. The HRD will respond to written questions within a reasonable time.
- b. Employees will be advised in writing when they need to complete background investigation forms because of their position risk designation.

9. **SUITABILITY.** This section sets out key requirements for determining suitability for covered positions as set forth more fully in 5 C.F.R. § 731. The provisions of the regulation should be consulted and followed when processing suitability matters. Although not required for positions that are not “covered positions” as defined above and in 5 C.F.R. § 731, the CSB applies the criteria outlined in 5 CFR Part 731.202 to *all* applicants and appointees at the CSB. Determinations made under this section are distinct from determinations of eligibility for assignment to, or retention in, sensitive national security positions made under E.O. 12968 or similar authorities.

- a. **Requirements.** Every position must be designated at a position risk level commensurate with the public trust responsibilities and attributes of the position, as they relate to the efficiency of the service. This is separate from determining position sensitivity for those positions in which the incumbent needs a security clearance for access to classified national security information. The suitability position risk levels are ranked according to the degree of adverse impact on the efficiency of the service that an unsuitable person could cause. The designated position risk or sensitivity levels are required on various personnel forms (e.g., the Position Description Optional Form (OF-8), the Notification of Personnel Action Standard Form (SF-50), and on the Request for Personnel Action Standard Form (SF-52). A position risk level is required for every position at the CSB.
- b. **Risk Designation System.** To determine position risk levels under this section, a Risk Designation System is used to assure that positions are designated uniformly and consistently throughout the CSB. (Refer to Appendix A for detailed guidance provided to agencies by OPM to assist with this process.) See also 5 C.F.R. 731.106 for additional information on the risk designation process.

1. Criteria

- A. Most employees can affect certain Government activities. Such activities include law enforcement, public safety and health, collection of revenue, and regulation of business, industry, or finance.
- B. Other Government activities, not by their nature having as great an impact upon the nation generally, include particular functions having the potential for damage. Positions having authority to commit Government funds through grants, loans, loan guarantees, or contracts would be public trust positions.
- C. Positions which are responsible for managing programs or operations require a high degree of public trust because of their ability to affect the accomplishment of the CSB's mission to a significant degree, including positions responsible for managing a significant portion of a CSB program.

2. Risk Levels – The three suitability position risk levels of High Risk (HR), Moderate Risk (MR) and Low Risk (LR) and their adverse impacts on the efficiency of the service are as follows:

- A. **HR (6) Public Trust Positions**, which have the potential for exceptionally serious impact, involving duties especially critical to the CSB or a program mission with broad scope or policy or program authority.
  - B. **MR (5) Public Trust Positions**, which have the potential for moderate to serious impact, involving duties of considerable importance to the agency or program mission, with significant program responsibilities and delivery of customer services to the public.
  - C. **LR (1) Positions**, which involve duties of limited relation to the agency mission, with program responsibilities that affect the efficiency of the service.
- c. **Investigative Requirements.** Persons receiving an appointment that is subject to investigation under 5 C.F.R. 731 must undergo a background investigation. **Investigations should be initiated before appointment but no later than 14 days after placement in the position.** See 5 C.F.R. § 731.106.

1. All employees at the CSB or from another agency selected for or moving to a position at a higher risk level than that previously occupied, must meet the investigative requirements of the new risk level (see Appendix A).
  2. If the risk level of the position itself is changed, the incumbent may remain in the position, but the investigation required by the new risk level must be initiated within 14 days by the HRD after re-designation is final.
  3. If an employee has received the required investigation for placement in the new risk level, no reinvestigation is required unless updating is considered necessary because of the time elapsed since the previous investigation, or because of other special circumstances which justify additional investigation (see Suitability Reinvestigation below).
- d. **Suitability Determinations.** In determining whether its action will promote the efficiency of the service, the CSB shall make its determination based on:
1. Whether the conduct of the individual may reasonably be expected to interfere with, or prevent, efficient service in the position applied for or employed in.
  2. Whether the conduct of the individual may reasonably be expected to interfere with, or prevent, effective accomplishment by the CSB of its duties or responsibilities; and,
  3. Whether a statutory or regulatory bar prevents the lawful employment of the individual in the position in question.
  4. When making a determination under this section, any of the following reasons may be considered a basis for finding an individual unsuitable:
    - A. Misconduct or negligence in prior employment that would have a bearing on efficient service in the position in question, or would interfere with or prevent effective accomplishment by the CSB of its duties and responsibilities;
    - B. Criminal conduct or dishonest conduct related to the duties to be assigned to the applicant or appointee, or to that person's service in the position or the service of other employees;
    - C. Material, Intentional false statement, deception, or fraud in examination or appointment;
    - D. Refusal to furnish testimony as required by Civil Service Rule 5.4;
    - E. Alcohol abuse of a nature and duration, which suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of others;
    - F. Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation;

G. Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force; or,

H. Any statutory or regulatory bar that prevents the lawful employment of the person involved in the position in question.

5. In making a determination under this section, the CSB will consider the following additional factors, to the extent that they are deemed pertinent to the individual case:

CONSIDERATION	GENERAL APPLICATION/DISCUSSION
1. The <b>NATURE OF THE POSITION</b> for which the person is applying or in which the person is employed.	The more authority, responsibility, sensitivity, and public trust associated with the position, the higher the risks involved and the more potential adverse impact there is to the efficiency and integrity of the service; thus the misconduct becomes more serious as a potentially disqualifying issue. However, certain kinds of conduct may result in disqualification regardless of the position.
2. The <b>NATURE AND SERIOUSNESS</b> of the conduct	The more serious the conduct, the greater the potential for disqualification.
3. The <b>CIRCUMSTANCES</b> surrounding the conduct.	Full facts and circumstances are essential to insure justice to the person and to protect the interests of the Government.
4. The <b>RECENCY</b> of the conduct.	The more recent the conduct is, the greater the potential for disqualification.
5. The <b>AGE</b> of the person at the time of the conduct.	Offenses committed as a minor are treated as less serious than those committed as an adult, unless the offense is very recent, part of a pattern, or particularly heinous.
6. Contributing <b>SOCIETAL CONDITIONS</b> .	Economic and cultural conditions might be a mitigating factor if the conditions are now removed. Generally considered in cases with relatively minor issues.
7. The absence or presence of <b>REHABILITATION</b> or efforts toward rehabilitation.	Clear, affirmative evidence of rehabilitation is required for a favorable determination. Rehabilitation may be a consideration for all conduct, not just alcohol and drug abuse. While formal counseling or treatment may be a consideration, other factors (such as the individual's employment record) may also be indications of rehabilitation.

e. **Record of Determination.** When the CSB exercising authority under this part by delegation from OPM, makes a suitability determination or changes a tentative favorable placement decision to an unfavorable decision, based on an OPM report of investigation or upon an investigation conducted pursuant to OPM-delegated authority, the CSB must:

1. Ensure that the records used in making the determination are accurate, relevant, timely, and complete to the extent reasonably necessary to ensure fairness to the person in any determination;
2. Ensure that all applicable administrative procedural requirements provided by law, the regulations in this part, and OPM issuances as described in Sec. 731.102(c) have been observed;
3. Consider all available information in reaching its final decision on a suitability determination or suitability action, except information furnished by a non-corroborated confidential source, which may be used only for limited purposes, such as information used to develop a lead or in interrogatories to a subject, if the identity of the source is not compromised in any way; and

4. Keep any record of the agency suitability determination or action as required by OPM issuances as described in 5 C.F.R. § 731.102(c).
- f. **Due Process.** If a suitability determination results in a decision by the CSB to withdraw an employment offer, or to remove an appointee or employee from the federal service, the procedures and appeal rights of either 5 CFR 731, Subparts D and E (Suitability), 5 CFR Part 315, Subpart H (Probationary Employees), or 5 CFR 752, Subparts D through F (Adverse Actions) will be followed, depending on the employment status of the Federal service applicant, appointee, or employee. Employees removed from Federal service are entitled to dispute this action using applicable appeal or complaint procedures available under Federal regulations.
- g. **Re-designation.** For the purpose of this Order, positions will be re-designated only as:
  1. They are filled,
  2. New positions are established,
  3. Position descriptions are revised,
  4. Reorganizations occur,
  5. There are IT or national security considerations; or
  6. Other significant factors, as determined by the Chairperson, merit re-designation.

NOTE: Positions that are already designated as documented in current position descriptions as of the date of the adoption of this order do not need to be re-designated unless one of the above factors applies.

- h. **Suitability Reinvestigation.** Every incumbent of a position designated at a HR IT (6C) level will be subject to a periodic reinvestigation 5 years after placement and at least once each succeeding 5 years. Regardless of a position risk or sensitivity level, a reinvestigation is also required if the individual had over a two-year break-in-service since the last investigation, even if that investigation was appropriate for the current position's risk level. See 5 C.F.R. § 731.106(d) for additional information.
- i. **Challenge to Risk Designation.**
  - A. When an employee is notified that there is a need to complete personal history forms because they have not met the background investigation requirement for their position's designated risk or sensitivity level, the employee may use the procedures in this section to challenge the risk designation of the position he/she occupies.
  - B. Documents concerning the risk designation may be requested within 2 workdays and shall be provided within 10 workdays from the HRD.

- C. Upon receipt of the risk designation information, the employee may file a reconsideration request, in writing, within 5 workdays to the HRD or his/her designee.
- D. The HRD will issue a written decision within 15 workdays after receipt of the reconsideration request.
- E. The employee shall have 5 workdays after receipt of the decision, to appeal in writing to the Chairperson or his/her designee.
- F. A final written decision will be issued within 30 workdays after receipt of the appeal by the Chairperson or designee.
- G. This decision is final and will not be subject to further agency review.
- H. The time frames in this appeal process may be extended, in writing, by the Chairperson.
- I. Except for an individual in his or her first year of service with the CSB, an employee who has filed an appeal will not be required to complete a personal history form until the above administrative process has been exhausted.
- J. If the HRD challenges a re-designation, the Chief of Personnel Security will fulfill the role of the HRD as set forth in this section.

10. **COMPUTER/IT RISK CRITERIA AND LEVELS.**

a. **Security of Federal Automated Information Systems.**

Appendix III of OMB Circular No. A-130, requires the Director of OPM to maintain personnel security policies for Federal personnel associated with the design, programming, operation, maintenance, or use of Federal automated information systems. The CSB is required to establish and manage personnel security policies and procedures to assure an adequate level of security for Federal automated information systems. In accordance with Appendix III of OMB Circular A-130, CSB policies and procedures for the security of Federal automated information systems must conform to the OPM guidance, which applies to all Federal employees.

Policies established and maintained by the CSB include requirements for screening all individuals (including contractors) participating in the design, development, operation, or maintenance of sensitive applications, as well as those having access to sensitive data. The level of screening required by these policies is to vary from minimal checks to full background investigations, depending on the sensitivity of the information to be handled and the risk and magnitude of loss or harm that the individual could cause.

b. **Risk Levels and Criteria**

The computer/IT risk levels and criteria are to be used as an integral part of Suitability Position Risk Designation Systems described in Appendix A. In determining position placement, in addition to public trust criteria, any position with computer/IT duties should have the following criteria applied.

1. Risk Levels

The three computer/IT position risk levels are as follows:

- a. **HR (6C) Public Trust Positions**, which have the potential for exceptionally serious impact involving duties especially critical to the CSB mission, with broad scope and authority, and with major program responsibilities that affect a major computer/IT system(s).
- b. **MR (5C) Public Trust Positions**, which have the potential for moderate to serious impact, involving duties of considerable importance to the CSB mission, and with significant responsibilities that affect large portions of a computer/IT system(s).
- c. **LR (1C) positions**, which have the potential for impact involving duties of limited relation to the CSB mission through the use of computer/IT system(s).

2. Criteria

- a. *High Risk (6C)* includes any position at the highest level of risk to the computer/IT system. This is to include positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way as to incur a relatively high risk of causing grave damage or realizing a significant personal gain. Such positions may involve:
  - Responsibility for the development and administration of the CSB's computer security programs, including direction and control of risk analysis and/or threat assessment.
  - Significant involvement in life-critical or mission-critical systems.
  - Responsibility for the preparation or approval of data for input into a system that does not necessarily involve personal access to the system, but has relatively high risk of effecting grave damage or realizing significant personal gain.



- Relatively high-risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of \$10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority to insure the integrity of the systems.
  - Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management - of systems hardware and software.
  - Other positions, as designated by the Chairperson, involving relatively high risk of effecting grave damage or realizing significant personal gain.
- b. *Moderate Risk (5C)* includes positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, whose work is technically reviewed by a higher authority at the HR (6C) level, to insure the integrity of the system. Such positions may involve:
- Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority at the HR (6C) level to insure the integrity of the systems. This level includes, but is not limited to:
    - Access to and/or processing of proprietary data, and Privacy Act of 1974 and Government-developed privileged information involving the award of contracts; and,
    - Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year.
  - Other positions, as designated by the Secretary, involving a degree of access to a system that creates a significant potential for damage or personal gain, but less than that in HR (6C) positions.
- c. *Low Risk (1C)* includes all computer/IT positions not falling into one of the above risk levels. In order to establish uniformity and objectivity, the CSB must make computer/IT risk designations in a systematic manner. Refer to instructions in Appendix A of this handbook and FPM chapter 731 and 732 for specific guidelines that may be applicable to the final designation.

Suitability Risk Level – Computer/IT Risk Level Inter-Relationships

As positions may involve determinations of risk levels for both suitability and computer/IT, the higher of the two is used to determine the possible adverse impact of the position and its final risk level.

11. **NATIONAL SECURITY POSITIONS.**

- a. For the purposes of this section, "National Security Position" includes positions in the CSB that require regular use of or access to classified information.
- b. **Applicability.** The requirements of this chapter apply to Board Members, competitive and excepted service positions, and to SES positions filled by career or non-career appointment employees within the CSB.
- c. **Adjudicative Guidelines.** The CSB follows adjudicative guidelines approved by the President on December 29, 2005 to determine an individual's eligibility for access to classified national security information. These guidelines are available for review at the following website: <http://www.archives.gov/isoo/pdf/hadley-adjudicative-guidelines.pdf>. All agencies are required to honor clearances granted under these guidelines, consistent with E.O. 12968.
- d. **Sensitivity Level Designation.** All positions that have national security duties must be designated at national security sensitivity levels to assure appropriate screening under E.O.12968. Sensitivity designation is based on an assessment of the degree of damage that an individual, by virtue of the occupancy of a position, could cause to the national security. The required investigation is conducted to provide a basis for insuring that employment of the individual is clearly consistent with the interests of the national security.
- e. **Risk Designation System.** To determine position sensitivity levels under this section, the Risk Designation System in Appendix A is used to assure that positions are designated uniformly and consistently. The national security criteria described in this section are used together with the risk designation system to arrive at the final position designation.

There are 2 sensitivity levels for designating positions for national security related positions. These levels and the degree of risk to the national security associated with each are indicated below.

Code	Sensitivity Levels	National Security Risk Criteria
3	Critical Sensitive (CS)	<p>Potential for exceptionally grave damage to the national security.</p> <p>Includes positions involving any of the following:</p> <ul style="list-style-type: none"> <li>• Access to Top Secret defense information;</li> <li>• Development or approval of war plans, plans or particulars of future or major or special operations of war;</li> <li>• Investigative duties, the issuance of personnel security clearances, or duty on personnel security boards; or</li> <li>• Other positions related to national security, regardless of duties, that require the same degree of trust.</li> </ul>

2	Non-Critical Sensitive (NCS)	<p>Potential for some damage to serious damage to the national security.</p> <p>Includes positions that involve one of the following:</p> <ul style="list-style-type: none"> <li>• Access to Secret or Confidential national security materials, information, etc.; or</li> <li>• Duties that may directly or indirectly adversely affect the national security operations of the agency.</li> </ul>
---	------------------------------	--

**Security Office Record on Sensitivity Designation, Access Level, and Investigative Requirement**

The HRD will complete the Position Designation Record form, which will become part of the CSB system of records. Please refer to Appendix C for more information. The HRD will maintain a record that includes some of the following information for each position in the CSB that has duties that require access to classified national security information:

<b>A. Sensitivity level of the position and coding for personnel documents under Section 9:</b>		
	<i>Level</i>	<i>Code*</i>
	3 Critical Sensitive (CS)	3
	2 Non-Critical Sensitive (NCS)	2
*Identify computer/IT positions with a "C" after the code.		
Include the completed Position Designation Record (see sample, Appendix C) in the record.		
<b>B. The position's level of access to classified information under Section 11:</b>		
	<i>Level</i>	<i>Code</i>
	Not Required	0
	Confidential (C - E.O. 12968)	1
	Secret (S - E.O. 12968)	2
	Top Secret (TS - E.O. 12968)	3
<b>C. Personnel background investigation requirement under Section 12:</b>		
	Special Background Investigation (SSBI)	
	Background Investigation (BI)	
	Limited Background Investigation (LBI)	
	Minimum Background Investigation (MBI)	

**f. Waiver Requirements.**

A. General: A waiver of the pre-appointment investigative requirement contained in E.O. 12968 for employment in a sensitive national security position may be made only for a limited period:

1. In the case of an emergency, if the Chairperson or his designee finds that such action is in the national interest; and

2. When such finding is made a part of CSB's records.

**B. Specific Waiver Requirements**

1. For positions designated Critical Sensitive, pre-appointment record checks must be conducted.
2. Requests for waivers may be initiated only when the performance of the CSB's mission is at risk. Workload, backlogs, or administrative problems caused by vacancies will not in themselves be sufficient basis for a waiver application.
3. When a waiver is authorized, the required investigation will be initiated within 14 days of placement of the individual in the position.

**g. Reciprocal Recognition of Existing Personnel Security Clearances**

- A. In accordance with the December 12, 2005 memorandum from the Office of Management and Budget, (see <http://www.archives.gov/isoo/pdf/omb-reciprocity-memo.pdf>), an individual with an existing security clearance (not including an interim clearance) who transfers or changes employment status is eligible for a security clearance at the same or lower level at the CSB without additional or duplicative adjudication, investigation, or reinvestigation, and without any requirement to complete or update a security questionnaire unless the CSB has substantial information indicating that the standards of Executive Order 12968 may not be satisfied.
  1. The “substantial information” exception to reciprocity of security clearances does not authorize requesting a new security questionnaire, reviewing existing background investigations or security questionnaires, or initiating new investigative checks (such as credit check) to determine whether such “substantial information” exists.
  2. The CSB may request copies of background investigations and/or security questionnaires from the existing or losing activity for purposes of establishing a personnel security file, but eligibility for a reciprocal security clearance may not be delayed nor may there be additional or duplicative adjudication after the documents are received.
  3. The HRD will verify with the existing or losing activity or its security authority, as appropriate, the level of and basis for the security clearance. Where possible, automated databases will be used to confirm security clearances.
  4. An employee will immediately be granted a security clearance at the CSB provided the previous investigation is not more than seven years old for

Top Secret, ten years old for Secret, or fifteen years old for Confidential. This does not negate the existing requirement to initiate reinvestigations in accordance with the national “Investigative Standards for Background Investigations for Access to Classified Information.”

- h. **Periodic Reinvestigation Requirements.** The incumbent of each position designated Critical Sensitive is subject to reinvestigation every 5 years, and incumbents of Non-Critical Sensitive positions are subject to reinvestigation every 10 years, for national security reasons. The results of this periodic reinvestigation will be used to determine whether the continued employment of the individual in a sensitive position is clearly consistent with the interest of the national security.
- i. **Due Process.** When the CSB denies a security clearance under this section, or when, as a result of information in a background investigation, changes a tentative favorable, placement or clearance decision to an unfavorable decision, the CSB will:
  - 1. Ensure that the records used in making the decision are accurate, relevant, timely, and complete to the extent reasonably necessary to assure fairness to the individual in any determination.
  - 2. Comply with all applicable administrative due process requirements, as provided by law, rule, or regulation or this order as described in subsection j.; and
  - 3. At a minimum, provide the individual concerned:
    - i. Notice of specific reason(s) for the decision.
    - ii. An opportunity to respond; and,
    - iii. Notice of appeal rights, if any.
  - 4. Consider all available information in reaching its final decision; and
  - 5. Keep any record of the agency action required by OPM.
- j. **Due Process Procedures.** Before an unfavorable security determination is finalized under this section, the individual against whom an unfavorable adjudication has been made shall have an opportunity to explain, refute and/or mitigate the actionable information that was used in making the unfavorable determination. Otherwise persons may be unjustly rejected or not selected because of mistaken identity, unfounded allegations, or because certain mitigating circumstances were not known to the adjudicator. Accordingly, the Chief of Personnel Security will:
  - 1. provide the person with a written Statement of Reasons (SOR) for the decision. The Chief of Personnel Security shall prepare a summary from the investigative file, but will not include information that: (1) is classified (i.e., Top Secret, Secret, or Confidential), even if the subject has a security clearance; (2) would reveal the identity of a source granted confidentiality; (3) is protected sensitive medical information as

denoted in 5 CFR 297.205; or (4) is otherwise exempt from release by the Privacy Act;

2. provide within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 522) or the Privacy Act (3 U.S.C. 552a), as applicable, any documents, records, and reports upon which a denial or revocation is based. If the decision was based on information contained in a background investigation file, the person shall be provided the investigative agency's address in order to request a copy of the investigative file;
3. inform the person of their right to be represented by counsel or other representative at their own expense;
4. provide the person with an opportunity to respond to the SOR, and to request a review of the negative adjudicative determination. The written response must be submitted within 45 days from the date the person received and signed for the SOR. (Upon request by the person and approval of the Chief of Personnel Security, if warranted, up to an additional 30 days may be granted. An additional extension may be granted if the person has promptly requested and not received the investigative file referenced above.) If the individual does not respond to the SOR, the person shall be notified that a timely response was not received, and their eligibility for access to classified information or performance of sensitive duties is hereby denied/revoked. The person shall also be informed that the decision is final and is not subject to further appeal;
5. if the person responds to the SOR, review the documentation provided by the person and make a final Personnel Security determination;
6. provide the person with a Letter of Decision (LOD) that shall include:
  - i. the reasons for the decision;
  - ii. the identity of the deciding authority;
  - iii. notice of the right to appeal an unfavorable adjudication decision to the Personnel Security Appeals Board (PSAB). The PSAB is a panel, appointed by the Chairperson, which shall be comprised of at least three members, two of whom shall be selected from outside the security field. **The identity of the members of the PSAB shall not be revealed.**
7. notify the person the person can appeal within 30 calendar days from the date the person received and signed for the LOD in one of two ways:
  - i. by written appeal directly to the PSAB. A written appeal should include any supporting material not already provided substantiating why the LOD should be overturned in addition to any written statement the person wishes to make; or
  - ii. by requesting to appear personally before an Administrative Hearing

Examiner, designated by the CSB, and to present relevant documents, materials, and information. The written results of the appearance and all relevant documentation shall then be sent by the Administrative Hearing Examiner to the PSAB.

8. the address to send the appeal to: Administrator, Personnel Security Appeals Board, Chemical Safety Board, 2175 K Street, N.W., Washington, D.C.; and
9. that if the person chooses not to appeal to the PSAB the determination made by the Chief of Personnel Security shall be the final decision and is not subject to further appeal.

**k. The Administrative Hearing Examiner and PSAB.**

1. The Administrative Hearing Examiner will notify the appellant of the time, date and place for the personal appearance, which generally will be held within 30 calendar days after the request. The personal appearance generally will be conducted at or near the appellant's duty station. At the appearance, the appellant will have an opportunity to present oral and documentary information on their own behalf. While the personal appearance is designed so that the appellant can represent themselves, the appellant may obtain legal counsel or other assistance at their own expense to be present at the appearance. Postponement of the personal appearance can be granted only for good cause.
2. The appellant should be prepared to address all of the security concerns and supporting adverse information. Also, all supporting documents should be organized and readily accessible for presentation to the Administrative Hearing Examiner presiding at the appearance and for use in answering questions. The Administrative Hearing Examiner presiding at the appearance will have already reviewed the investigative file. The appellant should be prepared to articulate the reason or reasons he or she believes that the LOD should be overturned. The hearing provides an opportunity to provide additional information and documentation when appropriate. Simply repeating information which is already part of the record should be avoided. The appellant will not have the opportunity to present or cross-examine witnesses. If the appellant wants the views of others presented, the appellant should obtain these views in writing (e.g., letters of reference, letters from medical authorities, affidavits, etc.) and present the documents to the Administrative Hearing Examiner. During the appearance, the appellant will be allowed to make an oral presentation and submit documentation. The appellant may be asked questions that should be answered clearly, completely, and honestly. The Administrative Hearing Examiner is not there to present the Government's security concerns but rather to listen to any explanations that the appellant may have concerning their case.
3. At the end of the personal appearance, the appellant will be given an opportunity to make a closing statement. The appellant should stress the highlights rather than review the entire case. The appellant should show how the weight of all available information

supports overturning the unfavorable personnel security determination. The Administrative Hearing Examiner will review the investigative file, consider the appellants comments and review any additional documentation submitted, and then make a recommendation to the Administrator, PSAB, as to whether the clearance, access, or employment in sensitive duties should be denied, revoked or reinstated. The Administrative Hearing Examiner will provide a written summary or recording of the personal appearance to the Administrator, PSAB.

4. The Administrator, PSAB, will provide the Administrative Hearing Examiners written summary or recording of the personal appearance and recommendation, along with the appeal documentation to the PSAB. The PSAB will consider the recommendation of the Administrative Hearing Examiner along with the investigative file and render a decision. The decision of the PSAB shall be in writing, and final.
5. A person who has been determined ineligible for a security clearance and access to classified or sensitive information cannot be reconsidered for a security clearance or assignment of sensitive duties for at least 12 months from the date of the final decision of denial or revocation.

## 12. **PERSONNEL INVESTIGATIONS.**

- a. **Public Availability of Investigative Files.** Investigative files are records subject to the Privacy Act and FOIA, and are made available to requestors in accordance with the provisions of those Acts. Requests for OPM investigative records can be submitted to OPM, Center for Federal Investigations Services, Boyers, PA 16018. For additional information on the web go to the following url:  
<http://www.opm.gov/extra/investigate/foiatips.asp>
- b. **Personnel Investigations Forms.** The following forms are to be completed to initiate Security/Suitability investigations. The form to be used is determined by the type of position, as indicated in the form title. The e-QIP SF 86, SF 85P, SF 85P-S, and SF 85, must be completed using the *Electronic Questionnaires for Investigations Processing* (e-QIP), a web-based system.
  - A. e-QIP SF-85, Questionnaire for Non-Sensitive Positions - Required for positions designated Low Risk (1/1C) (must be electronic version in e-QIP)
  - B. e-QIP SF-85P, Questionnaire for Public Trust Positions – Required for positions designated Moderate Risk (5/5C) and High Risk (6/6C) (must be electronic version in e-QIP)
  - C. e-QIP SF-85P-S, Supplemental Questionnaire for Selected Positions – Required for positions designated High Risk (6/6C) (must be electronic version in e-QIP)



- D. e-QIP SF-86, Questionnaire for National Security Positions – Required for positions designated Critical Sensitive (3/3C) and Non-Critical Sensitive (2/2C) (must be electronic version in e-QIP) SF-87, Fingerprint Chart.
- E. OF-306, Declaration for Federal Employment.
- F. Fair Credit Reporting Release – *Not needed for positions designated Low Risk (1/1C)*

An OF 612, Optional Application for Federal Employment, or a resume containing the same information must be submitted with each set of forms.

**Reporting to OPM.** The HRD must notify OPM when initiating an investigation under E.O. 10450, and shall report to OPM the action taken with respect to individuals investigated pursuant to E.O. 10450 no later than 90 days after receipt of the final report of the investigation.

- 13. **RECORDKEEPING.** The HRD shall be responsible for maintaining adequate records of any action taken pursuant to this Order, in accordance with applicable laws, regulations, and CSB policy.
- 14. **REVIEW AND UPDATE.** The HRD is responsible for reviewing this Order annually in consultation with the Chairperson and Office Directors of the CSB. The HRD shall complete such review and propose any changes to the Board no later than March 1<sup>st</sup> of each year.

## **CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD**

May 20, 2008.

## Appendix A – Risk Designation System

**Introduction.** Proper position designation is the foundation of an effective and consistent suitability program. It determines what type of investigation is required and how closely an individual is screened for a position. Additionally, as the level of authority and responsibility of a position become greater, character and conduct become more significant in deciding whether employment or continued employment would protect the integrity and promote the efficiency of the Federal service.

**Position Risk/Sensitivity Level Designation Records.** The HRD will maintain the official record of Public Trust suitability or National Security position sensitivity level designations that will include any adjustments made due to the impact of IT or access to classified information requirements. The Position Risk/Sensitivity Level Designation Records are subject to review by OPM during periodic appraisals of agency suitability programs, or on a case-by-case basis, to assure that agencies are considering all pertinent factors when designating positions relative to the integrity and efficiency of the service.

**The Risk Designation System.** The Risk Designation System is divided into three parts:

- **Program Designation.** (The agency identifies both the impact and scope of an agency or agency program as related to the integrity and efficiency of the service. This determines the “program designation.”)
- **Position Risk Designation Points.** (The agency determines the degree of risk that a position poses to the agency or an agency program as related to the integrity and efficiency of the service. Each of five risk factors is ranked; the higher the degree of risk, the higher the point value for the risk factor. The point values are totaled to provide the total “position risk designation points” for a position.)
- **Position Designation.** (The Program Designation and Position Risk Designation Points are applied to determine the risk level “position designation.”)

*At this point, any pertinent adjustments are made, including unique factors specific to positions as well as organizational factors, to provide uniformity of operation. When it is obvious that position designation will result in a higher risk level, the other steps may not be needed. Once these are completed, the agency decides the “final designation” of the position and the type of investigation to conduct.*

### FILLING OUT THE POSITION DESIGNATION RECORD

*(See Sample form in Appendix C)*

#### Program Designation

- **Program Designation.** The agency identifies both the impact and scope of an agency or agency program as related to the integrity and efficiency of the service. This determines the “program designation.”

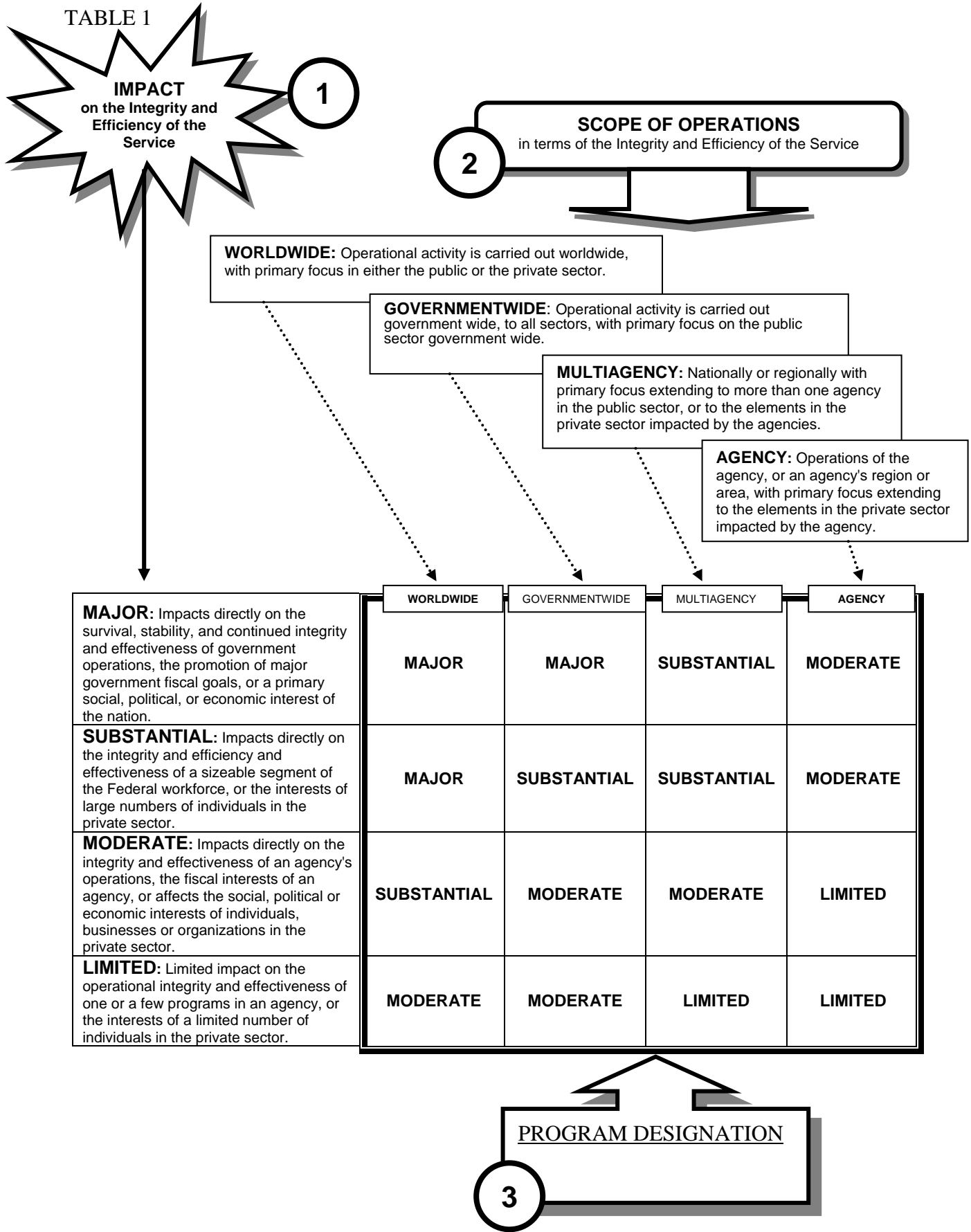
*Use these steps and Table 1 on the next page to complete part I –“Program Placement”*

- 1) Impact on the Integrity and Efficiency of the Service:** Identify the impact description in the IMPACT column of Table 1 that best describes the agency or agency program. If there is a question regarding the designation of an agency or agency program at one of two impact descriptions (such as whether it is *SUBSTANTIAL* or *MODERATE*), the decision should be based on the best interests of the agency mission.
- 2) Scope of Operations in Terms of the Integrity and Efficiency of the Service:** Identify the scope of operations described in the four SCOPE OF OPERATIONS columns of Table 1.
- 3) Determining Program Designation:** The box at the intersection of the IMPACT row and SCOPE column identifies the program designation.

**Examples:**

- ① SUBSTANTIAL IMPACT and ② MULTIAGENCY SCOPE = ③ *SUBSTANTIAL* Program Designation.
- ① LIMITED IMPACT and ② WORLDWIDE SCOPE = ③ *MODERATE* Program Designation.

TABLE 1



## Designating Position Risk Points

- **Position Risk Designation Points.** The agency determines the degree of risk that a position poses to the agency or an agency program as related to the integrity and efficiency of the service. Each of five risk factors is ranked; the higher the degree of risk, the higher the point value for the risk factor. The point values are totaled to provide the total “position risk points” for a position.

*Use these steps and Table 2 on the next page to complete part II –“Position Risk Designation Points”*

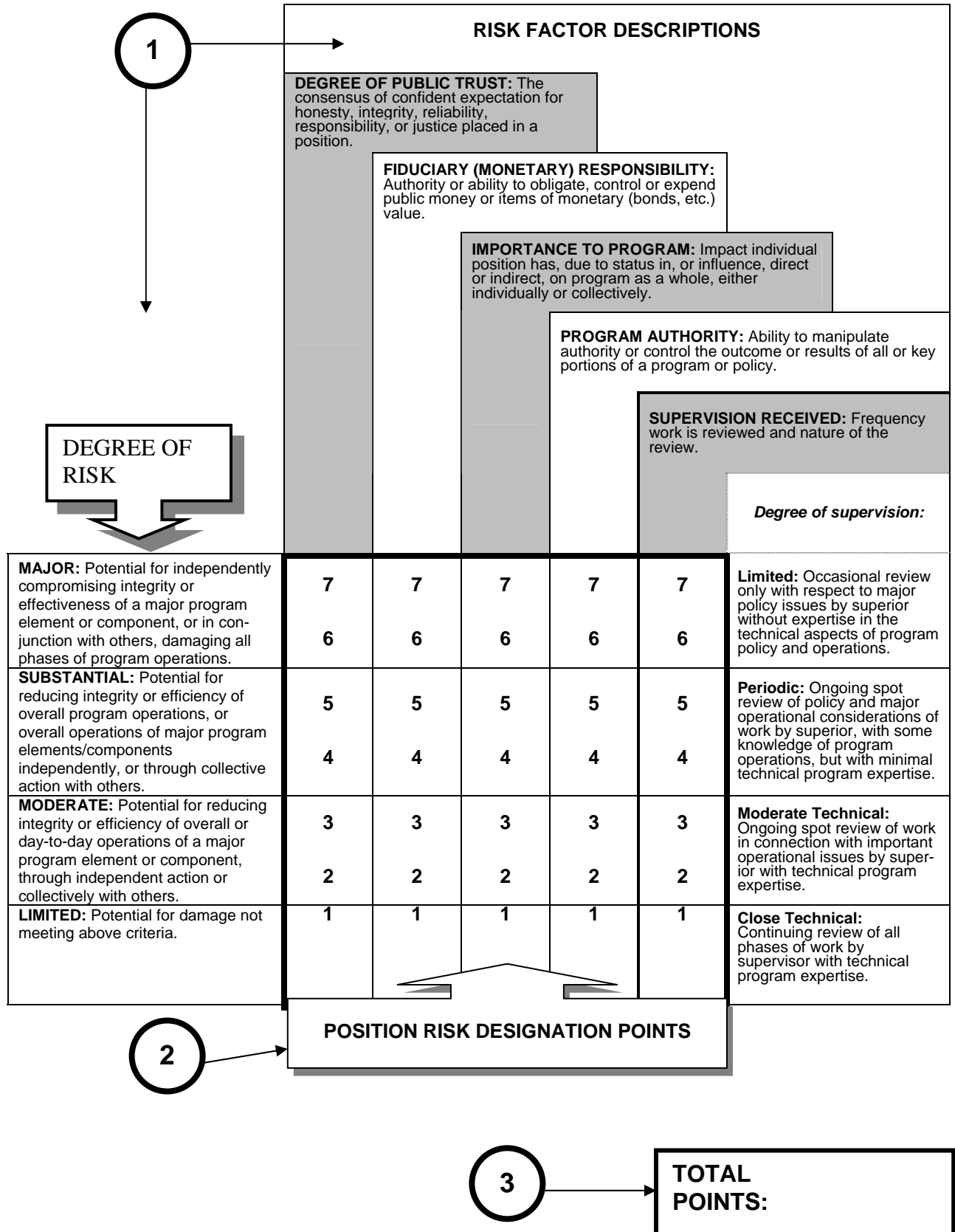
- 1) **Risk Factors and Degree of Risk:** Using a position description, or any documented information describing the duties and responsibilities of a position, evaluate each RISK FACTOR described at the top of Table 2 in terms of the DEGREE OF RISK described in the first column.
- 2) **Risk Factors and Points:** Assign points (7-6-5-4-3-2-1) to each risk factor to numerically reflect the DEGREE OF RISK. (The greater the degree of risk, the higher the point value assigned to the risk factor.)
- 3) **Total Points:** After points are assigned to all five risk factors, total the points. The result is a numerical representation of the relative degree of risk a position poses to the agency or an agency program (as related to the integrity and efficiency of the service).

### Example:

SUBSTANTIAL “Degree of Public Trust” = 5 points  
SUBSTANTIAL “Fiduciary (Monetary) Responsibility” = 4 points  
LIMITED “Importance to Program” = 1 point  
MODERATE “Program Authority” = 2 points  
MODERATE “Supervision Received” = 3 points

The total Position Risk Designation Points (5+4+1+2+3) = **15**

TABLE 2



## Position Designation

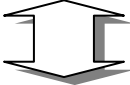
**Position Designation.** The Program Designation and Position Risk designation Points are applied to determine the risk level “position designation.”

*At this point, any pertinent adjustments are made, including unique factors specific to positions as well as organizational factors, to provide uniformity of operation. When it is obvious that position designation will result in a higher risk level, the other steps may not be needed.*

The results of part I, Program designation, and part II, Position Risk Designation Points, are next applied to Table 3 to determine the risk level of the position and to pair the risk level with the recommended minimum level of investigation for the position. The investigation recommendations are not intended to restrict an agency from conducting a more comprehensive investigation than that prescribed, when such investigation is considered warranted.

TABLE 3

		<b>II. POSITION RISK POINTS</b>					
<b>I. PROGRAM DESIGNATION</b>		5-10	11-17	18-23	24-29	30-33	34-35
<b>MAJOR</b>		Low Risk (LR) NACI	Moderate Risk (MR) LBI	Moderate Risk (MR) LBI	High Risk (HR) BI	High Risk (HR) BI	High Risk (HR) BI
<b>SUBSTANTIAL</b>		Low Risk (LR) NACI	Moderate Risk (MR) LBI	Moderate Risk (MR) LBI	Moderate Risk (MR) LBI	High Risk (HR) BI	High Risk (HR) BI
<b>MODERATE</b>		Low Risk (LR) NACI	Low Risk (LR) NACI	Moderate Risk (MR) MBI	Moderate Risk (MR) MBI	Moderate Risk (MR) LBI	High Risk (HR) BI
<b>LIMITED</b>		Low Risk (LR) NACI	Low Risk (LR) NACI	Low Risk (LR) NACI	Low Risk (LR) NACI	Moderate Risk (MR) LBI	High Risk (HR) BI



**POSITION RISK LEVEL AND TYPE OF BACKGROUND INVESTIGATION**

**Minimum Investigative Requirements.** The following are the **required** minimum levels:

LOW RISK - NACI  
 MODERATE RISK - MBI  
 HIGH RISK - BI

However, OPM recommends the levels shown in Table 3, above.

**Adjustments:** Some positions, by the very nature of the duties and responsibilities of the program or the position, will require designation at a certain level of risk. Final adjustment in the

designation process must take into account *unique* factors specific to positions, and the organizational need for *uniformity* of operations. Adjustments serve to raise the risk level designation of a position or convert the designation from a risk level to a sensitivity level. As a consequence, the level of investigation is often raised.

**Uniqueness.** Some factors that can cause a uniqueness adjustment, that are unique and are not fully accounted for in the program or position designation system, are listed here:

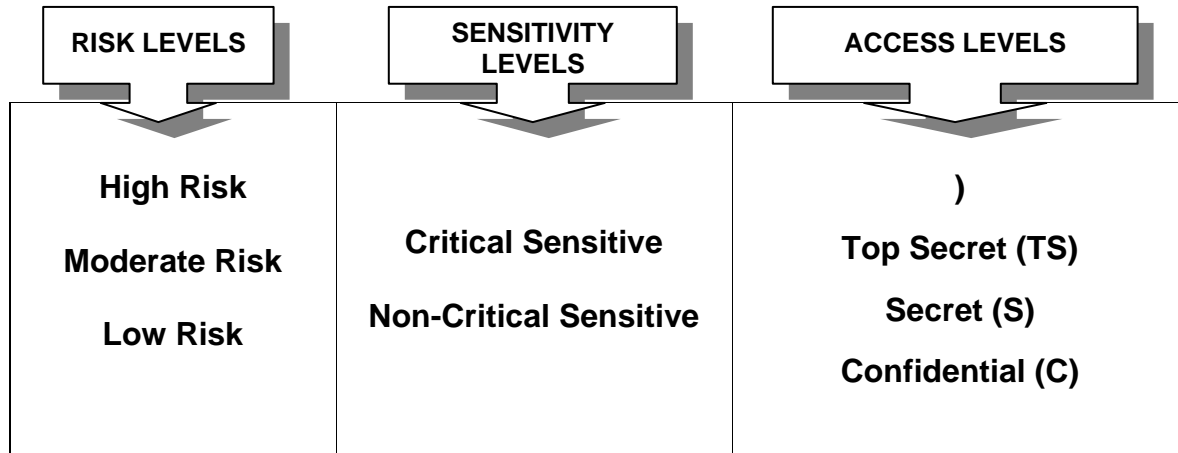
- Special investigative or criminal justice duties.
- Positions requiring possession and use of a firearm.
- Significant public health duties.
- Significant public safety duties.
- Access to or control of highly sensitive but unclassified information.
- Access to sensitive financial records.
- Potential for realizing significant personal gain.
- Control of an automated monetary system (such as key access entry).
- Few-of-a-kind positions with special duties (such as Special Assistant to Agency Head).
- Support positions with no responsibilities for preparation or implementation of Public Trust program policies and plans but involving regular contact with, and ongoing knowledge of, all or most of such material (such as Budget Analyst, Special Assistant).
- Any of the criteria appearing in 5 CFR 732 or E.O. 12968.
- Computer-ADP; any of the criteria under OMB Circular A-130 or the Computer Security Act of 1987.
- Any other factors the agency thinks relevant (these must be documented).

**Uniformity.** There may be a clearly indicated need for uniformity in position designations, because of authority level or program designation level; two examples that can cause adjustment are listed here:

- Agency head may adjust position designations at the same authority level to assure uniformity within the agency (for example, managers of major agency programs at the same level of authority may be designated at the same level of risk).
- If agency heads determine the designation levels of programs override and negate any specific risk considerations associated with individual positions within an agency or program, they may designate all positions within a program at the risk level required to protect the integrity and best promote the efficiency of the service.



Only after analysis of the position in terms of *uniqueness* and *uniformity* should any adjustment decision be made for FINAL DESIGNATION. FINAL DESIGNATION could be any one of the following:



**EXAMPLES:**

I. PROGRAM DESIGNATION	II. POSITION RISK DESIGNATION POINTS	III. POSITION DESIGNATION	MINIMUM INVESTIGATION	ADJUSTMENTS Uniqueness, Uniformity	FINAL DESIGNATION	REQUIRED INVESTIGATION
MODERATE	20	MR	MBI	Criminal Justice Duties	HR	BI
SUBSTANTIAL	29	MR	LBI	None	MR	LBI
MAJOR	25	HR	BI	TS Access (E.O. 12968)	CS	SSBI
MODERATE	30	MR	LBI	Special Assistant to Agency Head	HR	BI
MAJOR	25	HR	BI	5 CFR 732 (No Access)	CS	BI

Computer/IT Position Risk Levels – Refer to Chapter 2, Part VII for definitions and criteria for LR (1C), MR (5C), and HR (6C) IT positions.

## Appendix B – Form Investigation Matrix

### National Security Investigations

<b>Sensitivity Level</b>	<b>Investigative Form Used</b>	<b>Type of Investigation</b>
4 Special Sensitive	SF-86	SSBI
3 Critical Sensitive	SF-86	BI
2 Non-Critical Sensitive	SF-86	LBI or MBI

### Public Trust Investigations

<b>Risk Level</b>	<b>Investigative Form Used</b>	<b>Type of Investigation</b>
6 High Risk	SF-85P & SF 85P-S	BI
5 Moderate Risk	SF-85P	LBI or MBI
1 Low Risk	SF-85	NACI

Note: An OF-612 or a resume must accompany any request for investigation. If the OF-612 is submitted with an SF-85 or SF-85P, it must be updated to the date the SF-85 or SF-85P is signed.

The letter "C" will be added after the numerical risk level to denote IT responsibilities.

## Appendix C – Position Designation Record

The Chief of Personnel Security, in consultation with the HRD and Office of General Counsel, will complete the Position Designation Record form.

### POSITION DESIGNATION RECORD

POSITION TITLE: \_\_\_\_\_

POSITION DESCRIPTION #: \_\_\_\_\_

#### RISK DETERMINATION SYSTEM

##### I. PROGRAM PLACEMENT:

Impact on Efficiency of Service:	<u>N/A</u>
Scope of Operations for Efficiency of Service:	<u>N/A</u>
Placement (Major, Substantial, Moderate, Limited)	<u>Moderate</u>

##### II. POSITION PLACEMENT:

<u>Risk Factors</u>	<u>Risk Points</u>
a. Degree of Public Trust (7-1):	_____
b. Fiduciary Responsibilities (7-1):	_____
c. Importance to Program (7-1):	_____
d. Program Authority Level (7-1):	_____
e. Supervision Received (7-1):	_____
TOTAL POINTS	_____

##### III. POSITION PLACEMENT (HR: MR: LR):

Adjustments (Include Computer-IT Position Risk Criteria): Comments:

FINAL PLACEMENT (Risk level/Sensitivity level/Access level):

\_\_\_\_\_  
Signature of Agency Designator

\_\_\_\_\_  
Date